Laid-Open No.: 2003-0061666

Title: Traffic Collecting/Analyzing System and Method

Abstract:

Provided are a traffic collecting/analyzing system and a method thereof. More particularly, to a traffic collecting system that can collect and buffer all the packets transmitted/received in real-time while not affecting the speed of a network, separate them into a header and data, restore and store the user data into the original file by analyzing the header, process traffic statistically and store them, and allow an administrator to refer to the stored traffic, and a method thereof.

The present invention includes a packet collecting unit for collecting all packets transmitted/received on a network; a packet buffering unit for buffering and storing the packets collected in the packet collecting unit; a packet separating unit for separating each of the packets stored in the buffering unit into a packet header and user data; a packet analyzing and storing unit for analyzing the header of each packet, retrieving the user data into an original file, processing the traffic statistically, and storing the packet header and the restored user data; and an administrator consol for providing the restored user data and a function of referring to the traffic statistics.

The present invention has an advantage that when a company can properly cope with a security accident, such as leakage of confidential information, by registering what the information is about. Also, the stored information can be applied to other types of systems such as invasion detection system. An invasion shutdown system and the invasion detection system should be upgraded in preparation for new invasion patterns. However, the traffic collecting apparatus of the present invention can be operated regardless of the invasion pattern is new or not. Also, the present invention collects the generated traffic and the service starting/ending time of each IP by analyzing the header of an Internet Protocol (IP) packet on a network of an arbitrary IP. Therefore, it can be used quite usefully to figure out the data generated by one user's accessing the network from the service starting time to the service ending time. In addition, since the technology of the present invention operates a packet collecting engine and a packet processing server separately, it can minimize deterioration in their performance. Since it can store all data of packets, it can cope with processing the data collected in corporation with other systems flexibly and it can be expanded easily.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 12/56

(11) 공개번호 특2003-0061666
(43) 공개일자 2003년07월22일

(21) 출원번호 10-2002-0002339
(22) 출원일자 2002년01월15일

(71) 출원인 주식회사 아론통신기술
대한민국
305-806
대전 유성구 어은동 1번지 한국전자통신연구원 창업지원센타 5114호

(72) 발명자 강성준
대한민국
302-171
대전광역시서구갈마1동320-46

김도형
대한민국
300-080
대전광역시동구소제동299-7210/2

황재용
대한민국
302-727
대전광역시서구내동코오롱아파트6동1108호

한승희
대한민국
305-328
대전광역시유성구죽동49-1

(74) 대리인 최영규

(77) 심사청구 있음

(54) 출원명 트래픽 수집/분석 시스템 및 방법

요약

본 발명은 트래픽 수집/분석 시스템 및 방법에 관한 것으로, 특히 네트워크 속도에 영향을 미치지 않도록 하면서 실시간으로, 송/수신되는 모든 패킷에 대해 수집 및 버퍼링하며, 헤더와 사용자 데이터로 분리하며, 헤더 부분을 분석하여 사용자 데이터를 원래 파일로 복원 및 저장하며, 트래픽 통계 처리하여 이를 저장하며, 관리자가 조회할 수 있도록 하는 트래픽 수집 시스템 및 방법에 관한 것이다.

본 발명은, 네트워크상에 송/수신되는 모든 패킷을 수집하는 패킷 수집부; 상기 패킷 수집부에서 수집되는 패킷을 버퍼링하여 저장하는 패킷 버퍼링부; 상기 버퍼링부에 의해 저장되는 패킷을 패킷 헤더와 사용자 데이터로 분류하는 패킷 분류부; 상기 패킷 분류부에서 분류된 각 패킷의 헤더를 분석하여, 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 패킷 헤더와 상기 복원된 사용자 데이터를 저장하는 패킷 분석 및 저장부; 및 상기 복원된 사용자 데이터를 제공하고 트래픽 통계 조회 기능을 제공하는 관리자 콘솔을 포함하여 구성되는 것을 특징으로 한다.

본 발명은 기업 내 중요한 정보의 외부 유출에 대해 해당 정보가 무엇인지에 대해 기록 가능하여 보안 사고에 적절하게 대응할 수 있는 잇점이 있다. 또한 침입 탐지 시스템등과 같은 다른 종류의 시스템에서 상기 저장된 정보를 활용할 수 있다. 침입 차단 시스템이나 침입 탐지 시스템은 새로운 침입패턴에 대비하여 업그레이드 하지 않지 않으면 안되나, 본 발명의 트래픽 수집 장치는 새로운 침입패턴에 상관없이 동작 가능하다. 또한 본 발명은 임의의 IP(Internet Protocol) 네트워크상에서 IP 패킷의 헤더를 분석하여 각 IP별 서비스의 이용 시작/종료 시각, 발생 트래픽을 실시간으로 수집하여, 하나의 사용자가 네트워크에 접속하여 발생 시키는 데이터를 이용시작 시점부터 종료 시점까지 파악하는데 매우 유용하게 이용될 수 있다. 또한 본 발명은 패킷 수집 엔진과 패킷 처리 서버를 분리하여 가동하므로, 장비의 성능 저하를 최대한 방지하며, 패킷의 모든 데이터를 저장하므로 다른 시스템과의 연동에서 수집된 데이터를 통한 가공에 유연하게 대처하며 쉽게 확장이 가능하다.

대표도

도2

색인어

패킷 수집, 버퍼링, 패킷 조립, 네트워크 보안, 침입탐지

명세서

도면의 간단한 설명

도 1은 트래픽 수집/분석 시스템이 적용되는 전체 구성도.

도 2는 트래픽 수집/분석 시스템의 내부 구성을 도시한 블록도.

도 3은 전송되는 패킷의 데이터 포맷.

도 4는 패킷 버퍼링 동작을 나타내는 흐름도.

도 5는 패킷 분류 동작을 나타내는 흐름도.

도 6은 패킷 헤더 분석 절차를 도시한 흐름도.

도 7은 트래픽 통계 데이터 조회 절차를 도시한 흐름도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 트래픽 수집/분석 시스템 및 방법에 관한 것으로, 특히 네트워크 속도에 영향을 미치지 않도록 하면서 실시간으로, 송/수신되는 모든 패킷에 대해 수집 및 버퍼링하며, 헤더와 사용자 데이터로 분리하며, 헤더 부분을 분석하여 사용자 데이터를 원래 파일로 복원 및 저장하며, 트래픽 통계 처리하여 이를 저장하며, 관리자가 조회할 수 있도록 하는 트래픽 수집 시스템 및 방법에 관한 것이다.

종래의 네트워크 모니터링 시스템은 하나의 TCP/IP 패킷 플로우별로 트래픽 데이터를 수집함으로써, TCP 또는 UDP 접속에 대한 데이터만을 수집할 수가 있었다.

그러나, 네트워크 속도에 영향을 미치지 않도록 하면서 송/수신되는 모든 패킷을 수집하며 패킷의 헤더 부분을 분석하여 패킷의 사용자 데이터를 조립하고 원래 파일로 복원해 실시간으로 저장해 두면, 이렇게 저장된 정보들은 여러가지 목적으로 활용 가능하게 된다. 예를 들어, 네트워크 보안 분야에서 적용된다면, 기업내 중요한 정보의 외부 유출에 대해 해당 정보가 무엇인지에 대해 기록할 수가 있어서, 보안 사고에 적절하게 대응할 수가 있을 것이다.

인터넷과 네트워크 기술의 발달로 멀리 떨어진 컴퓨터도 LAN(Local Area Network)과 WAN(Wide Area Network)으로 연결해, 바로 옆에 있는 컴퓨터처럼 사용할 수 있게 되었으며, 필요로 하는 데이터도 쉽게 전송할 수 있게 되었다. 하지만, 이런 이점과는 달리 보안이 유지되는 정보의 유출, 불법침입에 의한 시스템 파괴 등도 또한 쉽게 이루어질 수 있는 문제점이 발생하게 되었다.

네트워크 보안 분야에서, 침입차단 시스템은 네트워크상에 존재하는 호스트들의 허가되지 않은 접근으로부터 내부 네트워크상에 존재하는 시스템들을 보호하기 위해 특정 서비스 및 네트워크 주소에 관련된 네트워크 접속만을 허용한다. 이러한 방식은 안정된 검사를 보장하며 물리적으로 내부 네트워크를 분리 시키는 장점이 있으나, 내부자 감시를 할 수 없고 네트워크 트래픽의 흐름을 가로막고 검사를 하므로 트래픽 속도를 지연시키며 낮은 대역폭에서만 적용 가능한 문제점이 있다. 침입탐지 시스템은 단순한 접근 제어 기능을 넘어서서, 네트워크상의 패킷 정보를 수집하고 침입패턴 데이터베이스를 참조하여 불법적인 침입 행위를 탐지한다.

그러나, 네트워크 보안을 위한 종래의 침입탐지 시스템은 패킷의 헤더 부분만을 분석함으로써, 네트워크 내부의 기밀이 유출되었을 경우 실제 어떤 데이터가 유출되었는지 정확히 알 수 없는 문제점이 있다. 실제로 메일을 통해 정상적인 사용자가 기밀 문서를 첨부하여 외부로 유출했다고 가정할 때, 이에 대한 정확한 근거제시를 하여, 보안 사고를 막을 수 있는 방법이 뚜렷하게 없는 실정이다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명의 목적은 네트워크 속도에 영향을 미치지 않도록 하면서 실시간으로 송/수신되는 모든 패킷을 수집 및 버퍼링하며, 패킷의 헤더 부분을 분석하여 패킷의 사용자 데이터를 조립하여 원래 파일로 복원해 실시간으로 저장하는 트래픽 수집 시스템 및 방법을 제공함에 있다.

본 발명의 다른 목적은 네트워크 속도에 영향을 미치지 않도록 하면서 실시간으로, 송/수신되는 모든 패킷에 대한 수집 및 버퍼링하며, 헤더와 사용자 데이터로 분리하며, 헤더 부분을 분석하여 사용자 데이터를 원래 파일로 복원 및 저장하며, 트래픽 통계 처리하여 이를 저장하며, 관리자가 조회할 수 있도록 하는 트래픽 수집 시스템 및 방법을 제공함에 있다.

이러한 목적을 달성하기 위한 본 발명은 네트워크상에 송/수신되는 모든 패킷을 수집하는 패킷 수집부; 상기 패킷 수집부에서 수집되는 패킷을 버퍼링하여 저장하는 패킷 버퍼링부; 상기 버퍼링부에 의해 저장되는 패킷을 패킷 헤더와 사용자 데이터로 분류하는 패킷 분류부; 상기 패킷 분류부에서 분류된 각 패킷의 헤더를 분석하여, 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 패킷 헤더와 상기 복원된 사용자 데이터를 저장하는 패킷 분석 및 저장부; 및 상기 복원된 사용자 데이터를 제공하고 트래픽 통계 조회 기능을 제공하는 관리자 콘솔을 포함하여 구성되는 것을 특징으로 한다.

그리고 본 발명은 네트워크상에 송/수신되는 모든 패킷을 수집하고, 상기 수집되는 패킷을 버퍼링하여 저장하며, 상기 버퍼링되어 저장되는 패킷을 전송하는 패킷 수집 엔진; 상기 패킷 수집 엔진으로부터 전송되어지는 패킷을 버퍼링하여 저장하며, 상기 버퍼링되어 저장되는 패킷을 헤더와 사용자 데이터로 분류하며, 상기 분류된 각 패킷의 헤더를 분석하여, 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 헤더와 상기 복원된 사용자 데이터를 저장하는 패킷 처리 서버; 및 상기 복원된 사용자 데이터를 오픈하여 제공하고 트래픽 통계 조회 기능을 제공하는 관리자 콘솔을 포함하여 구성되는 것을 특징으로 한다.

그리고 본 발명은 네트워크상에 송/수신되는 모든 패킷을 수집하는 제 1 단계; 상기 제 1 단계에서 수집되는 패킷을 버퍼링하여 저장하는 제 2 단계; 상기 제 2 단계에서 저장되는 패킷을 헤더와 사용자 데이터로 분류하는 제 3 단계; 상기 제

3 단계에서 분류된 각 패킷의 헤더를 분석하여, 상기 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 패킷과 상기 복원된 사용자 데이터를 저장하는 제 4 단계; 및 상기 복원된 사용자 데이터를 제공하고 트래픽 통계 조회 기능을 제공하는 제 5 단계를 포함하여 구성되는 것을 특징으로 한다.

발명의 구성 및 작용

이하 본 발명의 바람직한 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

도 1은 본 발명의 트래픽 수집 시스템이 적용되는 전체 구성도이다.

패킷 수집 엔진(103)은 내부 네트워크(115)로부터 외부 네트워크(101)(예:인터넷)로 송신되는 모든 패킷과, 외부 네트워크(101)로부터 내부 네트워크(115)로 수신되는 모든 패킷을 수집하여 이를 자체 데이터베이스에 버퍼링(Buffering) 하여 저장하고, 버퍼링되는 정보를 패킷 처리 서버(111)로 전송한다. 버퍼링하는 이유는 모든 패킷(헤더 부분 뿐만 아니라 사용자 데이터까지 포함된)에 대하여 실시간 수집하기 위해서이다.

패킷 수집 엔진(103)은 네트워크 인터페이스 카드(Network Interface Card), 랜 카드(LAN Card)등으로 구현 가능하다. 패킷 수집 엔진(103)의 네트워크 인터페이스를 Promiscuous 모드로 동작하도록 설정하여 내부 네트워크(103)상에 흘러 다니고 있는 모든 패킷을 수집하게 된다.

패킷 처리 서버(111)는 패킷 수집 엔진(103)으로부터 패킷 단위로 전송되어진 정보를 수신하고, 이를 버퍼링 하여 저장한다. 버퍼링 함으로써, 패킷 수집 엔진(103)에서 파일 전송 지연으로 인한 시스템 성능 저하를 사전에 방지한다. 패킷 처리 서버(111)에서는 패킷 단위로 정보를 읽어들여 각 패킷을 헤더와 사용자 데이터로 분리한다. 그리고 패킷 처리 서버(111)는 그 헤더를 분석(목적지 주소, 소오스 주소, 파일 종류(FTP, 메일등), 시퀀스 번호를 참조)하여 패킷을 조립하고 원패 사용자 데이터 파일로 복원하며, 또한 상기 헤더 분석을 통해 통계파일 작성을 위한 처리를 한 후 통계데이터를 저장한다. 그리고, 패킷 처리 서버(111)는 상기 분리된 헤더와 사용자 데이터를 저장한다.

이로 인해, 내부 네트워크(115) 속도에 영향을 미치지 않도록 하면서 실시간으로, 송/수신되는 모든 패킷의 헤더 정보 뿐만 아니라 사용자 데이터 까지도 손실없이 얻을 수 있게 되며, 관리자는 관리자 콘솔(113)의 조회 기능을 통해, 내부 네트워크(115)에서 들어오고 나가는 메일, FTP등 모든 정보들을 감시 및 저장할 수 있게 되며 통계 데이터를 확인할 수 있다.

도 2는 본 발명에 따른 트래픽 수집 시스템의 내부 구성을 도시한 블록도이다. 이하, 상기 도 1을 참조하여 설명하기로 한다.

패킷 수집 엔진(103)은 내부 네트워크(115)상에 흘러다니고 있는 모든 패킷을 수집하는 패킷 수집부(201), 수집된 패킷을 버퍼링하여 데이터베이스(207)에 저장하는 패킷 버퍼링부(203) 및 데이터베이스(207)에 버퍼링되는 패킷을 패킷 처리 서버(111)로 전송하는 패킷 전송부(205)로 구성된다.

패킷 수집부(201)는 유입되는 패킷을 모두 수집하거나, 또는 그 중 필요한 패킷들만 선택적으로 수집할 수가 있다. 패킷 수집부(201)는 포트 기반 패킷 선택, IP(Internet Protocol) 어드레스 기반 패킷 선택, 포트 & IP 어드레스 기반 패킷 선택, 전송 프로토콜별 선택등을 통하여 필요한 패킷을 선택적으로 수집하게 된다. 그리고 패킷 수집부(201)는 상기 수집된 패킷을 패킷 버퍼링부(203)로 전달한다.

패킷 버퍼링부(203)는 상기 패킷 수집부(201)로부터 전달받은 패킷들을 데이터베이스(207)에 버퍼링하여 저장한다. 이때, 패킷 버퍼링부(203)는 각 패킷의 앞 부분에 패킷 길이 정보를 첨부하고 파일로 저장할 수가 있는데, 하나의 디렉토리에 순차적으로 번호를 붙여서 파일을 생성한 후 기설정된 시간(예:1분당)동안에 전달되는 패킷을 연속적으로 파일에 저장한다. 패킷 버퍼링부(203)는 이렇게 일정한 시간이 지나면 패킷을 저장하고 있던 파일을 닫고, 다음 번호의 파일에 전달되는 패킷을 저장하게 된다. 이렇게 생성된 파일들이 미리 설정한 개수가 되면, 패킷 버퍼링부(203)는 맨 처음에 생성된 파일부터 삭제하면서 다시 새로운 파일을 생성하고 전달되는 패킷을 저장한다.

패킷 전송부(205)는 데이터베이스(207)에 버퍼링되는 패킷을 소켓을 통해 패킷 처리 서버(111)로 전송한다. 이때, 패킷 전송부(205)는 소정 시간(예:1초) 간격으로 데이터베이스(207)에 파일이 생성되어 있는지를 검사한다. 파일이 생성되어 있으면, 패킷 전송부(205)는 상기 첨부하여둔 패킷의 길이 만큼 파일을 읽어들여, 패킷 처리 서버(207)로 전송한다. 파일이 데이터베이스(207)에 생성되어 있지 않거나 또는 생성되어 있더라도 해당 파일에 패킷이 미처 다 저장되어 있지 않아 파일이 클로우즈(Close) 되어 있지 않으면, 패킷 전송부(205)는 대기 상태가 된다. 전송되는 패킷의 구조는 도 3과 같다. 패킷 전송부(205)는 소켓 통신을 이용하여 패킷을 전송할 수가 있는데, 만약 패킷 처리 서버(111)와의 소켓 인터페이스가 끊어지게 되면, 패킷 전송부(205)는 반복해서 소켓 연결을 시도하고, 소켓이 연결되면 다시 파일을 전송한다.

패킷 처리 서버(111)는 패킷 수집 엔진(103)으로부터 전송되어진 패킷을 입력 받아서 데이터베이스(211)에 버퍼링하여 저장하는 패킷 입력/버퍼링부(209)와, 데이터베이스(211)에 버퍼링되는 각 패킷을 헤더 부분과 사용자 데이터 부분으로 분류하는 패킷 분류부(213)와, 분류된 각 패킷의 헤더 부분을 분석하여 사용자 데이터 부분을 조립하고 이를 원래의 파일로 복원하며, 트래픽 통계 처리를 수행하여 트래픽 통계 정보를 저장하고 상기 분류된 각 패킷의 헤더 부분과 사용자 데이터 부분을 저장하는 패킷 분석/저장부(215)로 구성된다.

패킷 입력/버퍼링부(209)는 패킷 수집 엔진(103)의 패킷 전송부(205)로부터 전송되는 패킷을 입력 받아서 데이터베이스(211)에 버퍼링하여 저장한다. 패킷 입력/버퍼링부(209)는 패킷이 수신되면(401), 수신된 패킷이 설정된 개수(예:10000개) 이상인지를 검사한다(403). 수신된 패킷이 설정된 개수 이상이 아니면, 패킷 입력/버퍼링부(209)는 수신 패킷을 파일에 저장한다(405). 수신된 패킷이 설정된 갯수 이상이면, 패킷 입력/버퍼링부(209)는 저장중인 파일을 닫고 새로운 파일을 생성한다(407). 그리고 패킷 입력/버퍼링부(209)는 수신 패킷을 새로운 파일에 저장한다(405).(도 4 참조)

패킷 분류부(213)는 데이터베이스(211)에 버퍼링되는 각 패킷을 헤더 부분과 사용자 데이터 부분으로 분류한다. 패킷 분류부(213)는 데이터베이스(211)에 파일 저장 디렉토리를 생성하고(501), 버퍼링되는 ./file 디렉토리를 설정된 시간(예:10초)마다 모니터링 한다(503). 그리고 패킷 분류부(213)는 존재하는 파일이 설정 개수(예:10,000개)의 패킷이 저장 완료된 것이면, 해당 파일을 오픈한다(507). 이렇게 해서 오픈된 파일로부터 각 패킷에 첨부되어 있는 길이정보 만큼씩 데이터를 읽어 들이면, 이 데이터는 하나의 완전한 패킷의 구조를 갖게 된다. 패킷 분류부(213)는 각 패킷의 IP 헤더를 추출하여(509), 패킷이 TCP(Transport Control Protocol) 프로토콜에 해당하면(511), 패킷으로부터 TCP 헤더와 사용자 데이터를 추출한다(513).(도 5 참조)

패킷 분석/저장부(215)는 분류된 각 패킷의 헤더 부분을 분석한다. 그리고 상기 분석을 통해, 패킷별 사용자 데이터 부분을 조립하여 이를 원래의 파일로 복원한다. 또한 패킷 분석/저장부(215)는 상기 분석을 통해, 관리자가 일별, 월별 또는 지정한 기간 및 시간의 통계를 검색할 수 있도록, 트래픽 통계 처리를 수행하여 트래픽 통계 정보를 저장한다. 또한 패킷 분석/저장부(215)는 상기 각 패킷의 헤더 부분과 복원된 사용자 데이터 부분을 저장한다.

패킷 분석/저장부(215)는 트래픽 통계 파일의 크기가 너무 커지지 않고, 관리하기 편리 하도록 매일 한 개의 파일을 생성하게 되는데, 00시 00분을 기준으로 날짜가 변경되면(601), 새로운 트래픽 통계 파일을 생성하여(603), 트래픽 통계 데이터를 저장 한다. 날짜가 변경되지 않으면(601), 당일 생성되어있는 파일에 트래픽 통계 데이터를 저장한다.

패킷 분석/저장부(215)는 패킷의 헤더 부분을 분석한 결과, Finish 패킷이면(605), 할당된 Memory 공간을 초기화 하여 다시 사용할 수 있게 하고, Finish 패킷이 아니면(605), 수신 시간 초과 여부를 검사한다(609).

참고적으로 상기 609단계를 수행하는 이유를 설명하면, 일반적으로 송신측에서 어떤 파일이나 데이터를 전송할 때 컴퓨터는 이 파일이나 데이터를 네트워크 상태나 컴퓨터가 보낼 수 있는 크기로 분할하여 분할된 각각의 데이터에 헤더를 붙여서 전송하게 되는데, 이때 수신측 컴퓨터는 송신측에서 보낸 파일이나 데이터의 끝이 어디인지 알 수가 없기 때문에 이것을 구분할 수 있도록 하기 위하여 송신측에서는 보내는 마지막 패킷의 헤더에 Finish 패킷이라고 특정 플래그(구분자)를 기록하여 전송하기 때문이다.

한편, Finish 패킷 검사를 통해서 해당 파일의 수신이 완료되었는지 판단하게 되는데 패킷의 전송 도중 Finish packet이 오류나 기타 문제 때문에 수신되지 않는 경우가 있다. 이때 수신측에서 이 패킷을 기다리기 위해 할당된 메모리 공간을 초기화 하지 않는다면 시간이 지날수록 메모리 공간이 줄게 되어 시스템이 정지하는 경우가 발생된다. 이것을 방지하기 위해 수신 대기 시간을 설정해 놓고 이 시간 내에 Finish 패킷이 수신되지 않을 경우(609), 비정상 종료 처리를 하여 사용하고 있던 메모리 공간을 초기화 하고(611), 다시 사용할 수 있게 한다.

수신되는 수많은 패킷들은 각기 다른 파일의 데이터들이다. 즉, 한 네트워크 라인에는 수많은 사람들이 동시에 사용하고 있기 때문에 각기 다른 목적의 데이터들이 혼재하고 있다 이.시스템에서는 이러한 패킷들 중에 같은 파일에서 분리된 패킷들끼리 모아서 하나의 파일로 재결합해 놓아야 한다. 이때 같은 파일에서 분리된 패킷들 중 맨 처음 수신된 패킷이면(613), 이 패킷에 대한 헤더와 데이터를 저장할 파일을 오픈 한다(615). 이미 해당 파일이 오픈된 상태이면(613), 현재 사용하고 있는 메모리에 추가한다(617).

패킷 분석/저장부(215)는 상기와 같은 패킷 헤더 부분을 분석이 완료되면, 트래픽 통계 결과 파일을 저장한다(621).

본 발명의 실시예에서, 트래픽 통계 분석을 위해 필요한 항목은 하기 <표 1>과 같다.

[표 1]

항 목	의 미
NO	트래픽 통계 파일에 Writing 횟수(1씩 증가)
Packets	총 패킷 개수(1000개 단위 증가)
Files	현재 생성된 총 파일 수(누적)
Normal	현재 생성된 정상 종료 파일 수(누적)
Abnormal	현재 생성된 비정상 종료 파일 수(누적)
Open	현재 오픈되어 있는 파일 수
Time(sec)	입력 시간(UNIX TIME)

하기 <표 2>는 본 발명의 실시예에 따라 트래픽 통계 데이터가 파일에 저장되는 일 예를 보여준다.

[표 2]

NO	Packets	Files	Normal	Abnormal	Open	Times
1	1000	310	302	0	8	989506827
2	2000	619	611	0	8	989506857
3	3000	942	935	0	7	989506888
4	4000	1256	1248	0	8	989506914
5	5000	1582	1574	0	8	989506970
6	6000	1905	1897	0	8	989506997
7	7000	2214	2208	0	6	989507031
8	8000	2529	2521	0	8	989507078
9	9000	2833	2831	0	2	989507112
10	10000	3138	3134	0	4	989507159

패킷 분석/저장부(215)는 분류된 각 패킷의 헤더 부분과 사용자 데이터 부분(원래의 파일로 복원된)을 데이터베이스(211)에 저장한다.

관리자 콘솔(113)은 데이터베이스(211)에 저장된 사용자 파일을 오픈하여 관리자에게 제공하며, 데이터베이스(211)에 저장된 트래픽 통계 데이터를 조회할 수 있도록 한다. 트래픽 통계 결과는 파일 형식으로 저장되는데, 관리자가 필요한 데이터를 올바르게 입력하면(701, 703), 관리자 콘솔(113)은 해당되는 트래픽 통계 데이터 파일을 오픈하고, 필요한 기간동안의 트래픽 통계 결과를 계산하며 결과를 출력한다(705, 707, 709, 711).

하기 <표 3>은 트래픽 통계 데이터의 조회를 위해, 관리자가 입력 시키는 값의 일 예를 나타낸다.

[표 3]

	년/월/일	시/분/초
시작 시간	20010501	010100
종료 시간	20010531	240000

상기 도 2에서, 데이터베이스(211)는 침입 탐지 시스템(도시하지 않음.)에 연결될 수 있다. 데이터베이스(211)에는 네트워크(115) 상에 송/수신되는 패킷의 헤더 부분이 저장되게 되는데, 상기 침입 탐지 시스템의 헤더 분석을 위해 사용되어 진다. 본 발명의 트래픽 수집/분석 시스템은 침입 탐지 시스템의 서브 시스템으로도 활용 가능하다.

본 발명의 실시예에서는, 트래픽 수집/분석 시스템이 패킷 수집 엔진(103)과 패킷 처리 서버(111)로 분리되어 있는 구성이다. 이는 제어부(CPU)를 들로 나누어서 부하를 분배하며, 패킷 수집 엔진(103)이 네트워크(115)상에 송/수신되는 패킷을 놓치지 않고 수집하도록 하기 위함이다.

발명의 효과

따라서, 본 발명은 네트워크 속도에 영향을 미치지 않도록 하면서 실시간으로, 송/수신되는 모든 패킷에 대한 수집하고 이를 버퍼링하며 헤더와 사용자 데이터로 분리하며, 헤더 부분을 분석하여 사용자 데이터를 원래 파일로 복원 및 저장하며, 트래픽 통계 처리하여 이를 저장하며 관리자가 조회할 수 있도록 하여, 저장되는 정보들은 여러 가지 분야에서 활용 가능하게 된다. 예를 들어, 기업 내 중요한 정보의 외부 유출에 대해 해당 정보가 무엇인지에 대해 기록 가능하여 보안 사고에 적절하게 대응할 수 있는 잇점이 있다. 또한 침입 탐지 시스템등과 같은 다른 종류의 시스템에서 상기 저장된 정보를 활용할 수 있다. 침입 차단 시스템이나 침입 탐지 시스템은 새로운 침입패턴에 대비하여 업그레이드 하지 않지 않으면 안되나, 본 발명의 트래픽 수집 장치는 새로운 침입패턴에 상관없이 동작 가능하다.

또한 본 발명은 임의의 IP(Internet Protocol) 네트워크상에서 IP 패킷의 헤더를 분석하여 각 IP별 서비스의 이용 시작/종료 시각, 발생 트래픽을 실시간으로 수집하여, 하나의 사용자가 네트워크에 접속하여 발생 시키는 데이터를 이용시작 시점부터 종료 시점까지 파악하는데 매우 유용하게 이용될 수 있다.

또한 본 발명은 패킷 수집 엔진과 패킷 처리 서버를 분리하여 가동하므로, 장비의 성능 저하를 최대한 방지하며, 패킷의 모든 데이터를 저장하므로 다른 시스템과의 연동에서 수집된 데이터를 통한 가공에 유연하게 대처하며 쉽게 확장이 가능하다.

(57) 청구의 범위

청구항 1.

네트워크상에 송/수신되는 모든 패킷을 수집하는 패킷 수집부;

상기 패킷 수집부에서 수집되는 패킷을 버퍼링하여 저장하는 패킷 버퍼링부;

상기 버퍼링부에 의해 저장되는 패킷을 패킷 헤더와 사용자 데이터로 분류하는 패킷 분류부;

상기 패킷 분류부에서 분류된 각 패킷의 헤더를 분석하여, 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 패킷 헤더와 상기 복원된 사용자 데이터를 저장하는 패킷 분석 및 저장부; 및

상기 복원된 사용자 데이터를 제공하고 트래픽 통계 조회 기능을 제공하는 관리자 콘솔

을 포함하여 구성되는 것을 특징으로 하는 네트워크 트래픽 수집 및 분석 시스템.

청구항 2.

네트워크상에 송/수신되는 모든 패킷을 수집하고, 상기 수집되는 패킷을 버퍼링하여 저장하며, 상기 버퍼링되어 저장되는 패킷을 전송하는 패킷 수집 엔진;

상기 패킷 수집 엔진으로부터 전송되어지는 패킷을 버퍼링하여 저장하며, 상기 버퍼링되어 저장되는 패킷을 헤더와 사용자 데이터로 분류하며, 상기 분류된 각 패킷의 헤더를 분석하여, 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 헤더와 상기 복원된 사용자 데이터를 저장하는 패킷 처리 서버; 및

상기 복원된 사용자 데이터를 오픈하여 제공하고 트래픽 통계 조회 기능을 제공하는 관리자 콘솔

을 포함하여 구성되는 것을 특징으로 하는 네트워크 트래픽 수집 및 분석 시스템.

청구항 3.

네트워크상에 송/수신되는 모든 패킷을 수집하는 제 1 단계;

상기 제 1 단계에서 수집되는 패킷을 버퍼링하여 저장하는 제 2 단계;

상기 제 2 단계에서 저장되는 패킷을 헤더와 사용자 데이터로 분류하는 제 3 단계;

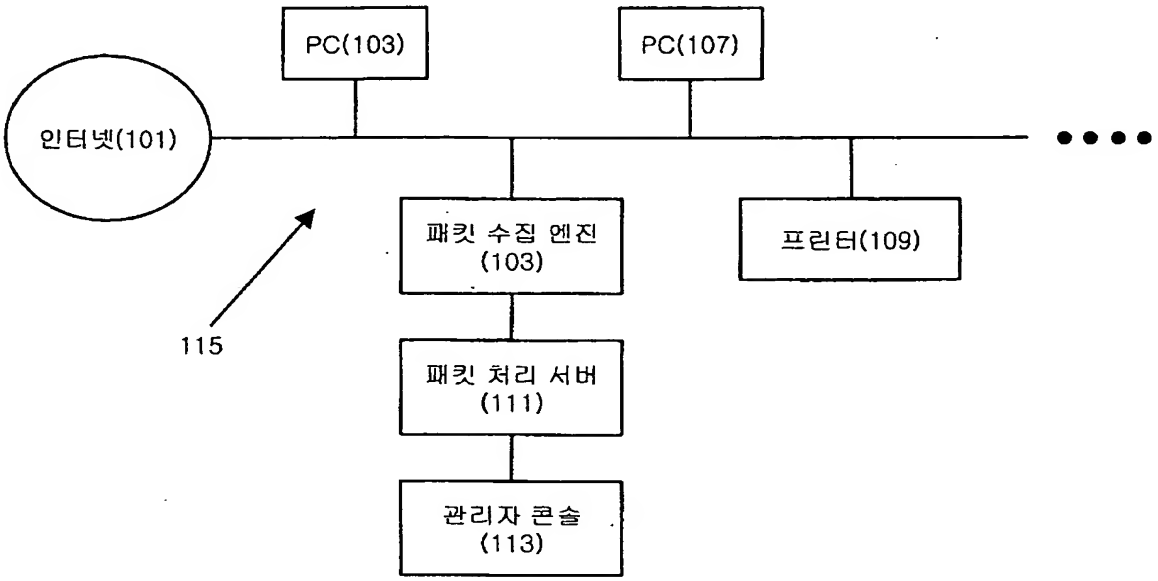
상기 제 3 단계에서 분류된 각 패킷의 헤더를 분석하여, 상기 사용자 데이터를 조립하여 원래의 파일로 복원하고 트래픽 통계처리를 수행하며, 상기 분류된 패킷과 상기 복원된 사용자 데이터를 저장하는 제 4 단계; 및

상기 복원된 사용자 데이터를 제공하고 트래픽 통계 조회 기능을 제공하는 제 5 단계

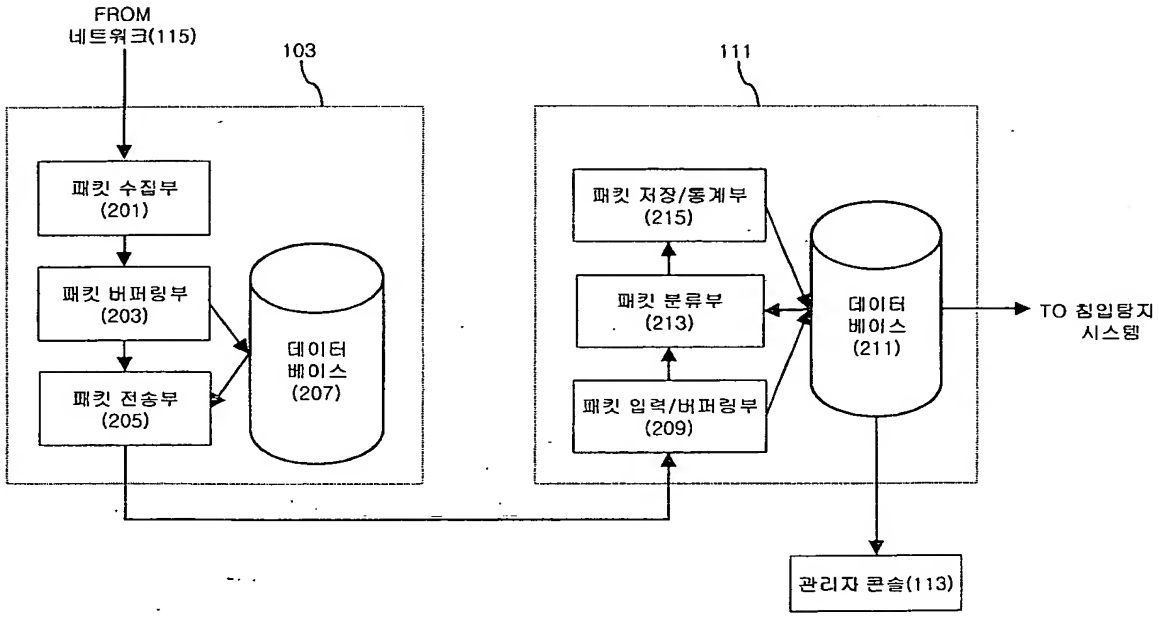
를 포함하여 구성되는 것을 특징으로 하는 네트워크 트래픽 수집 및 분석 방법.

도면

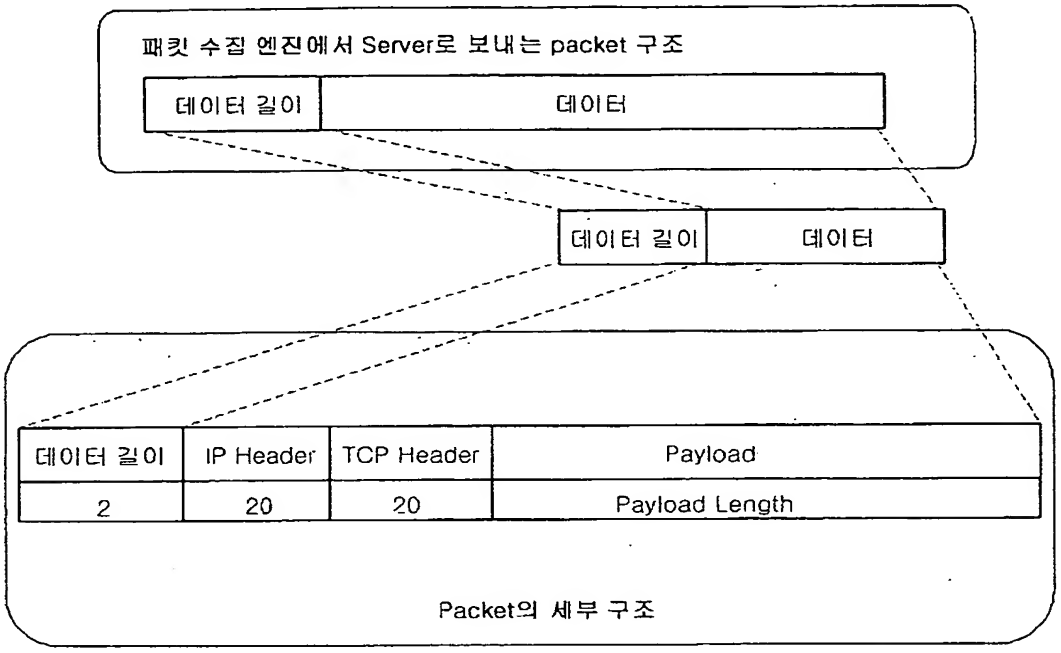
도면 1



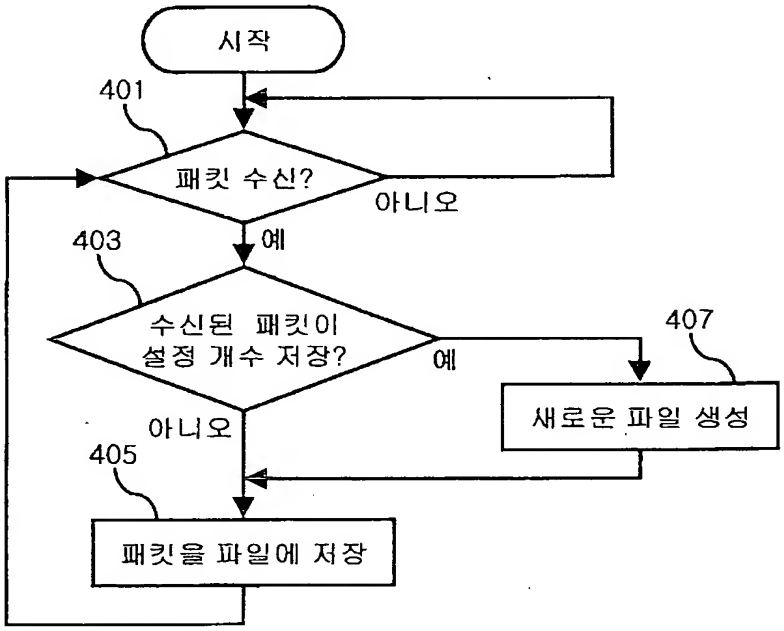
도면 2



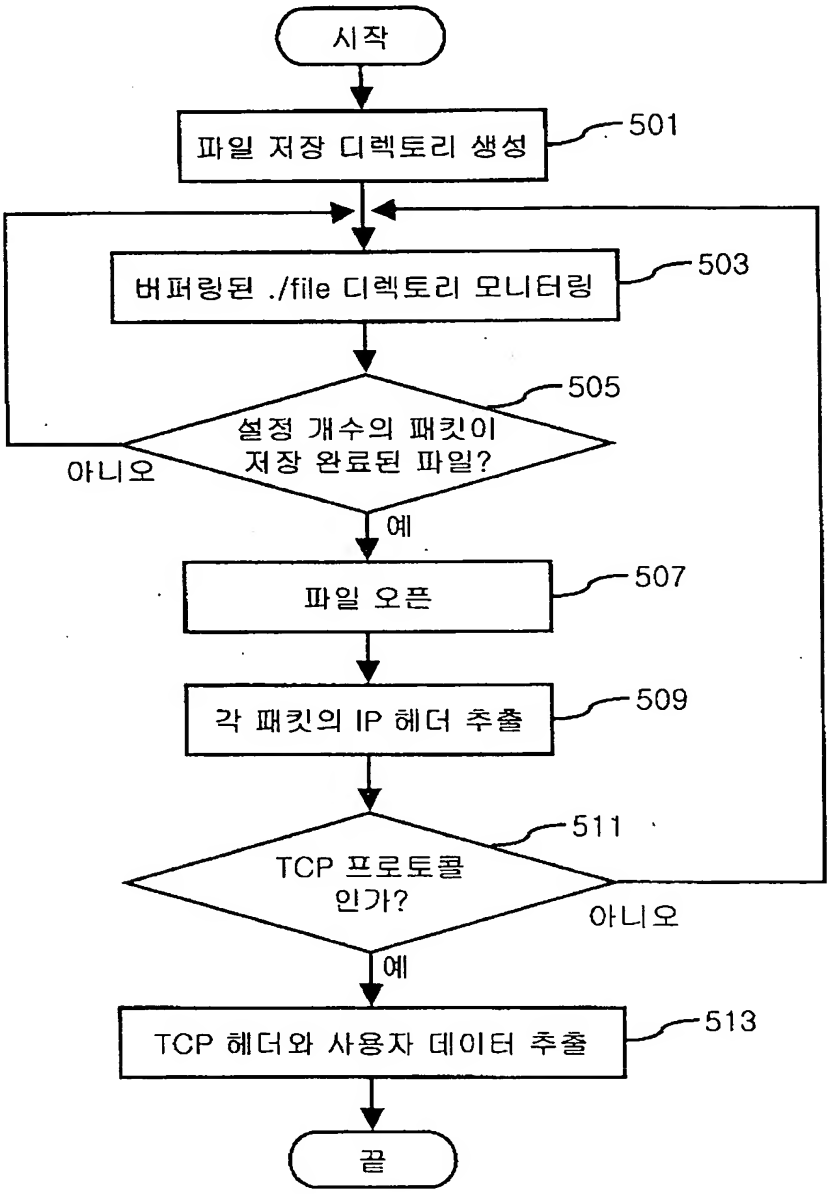
도면 3


패킷 수집 엔진에서 Server로 보내는 packet 구조
데이터 길이
데이터
데이터 길이
데이터
데이터 길이
IP Header
TCP Header
Payload
2
20
20
Payload Length
Packet의 세부 구조

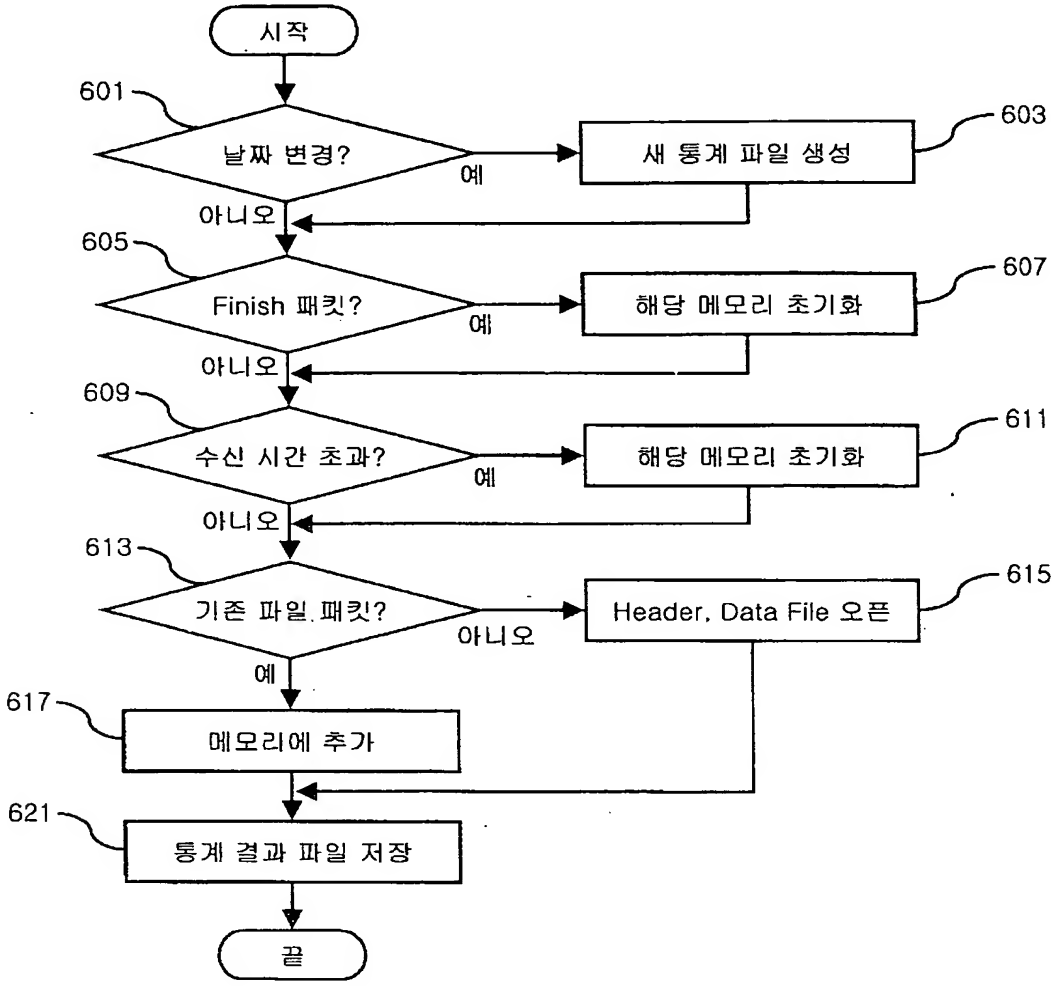
도면 4


시작
401
패킷 수신?
아니오
예
403
수신된 패킷이
설정 개수 저장?
예
407
새로운 파일 생성
아니오
405
패킷을 파일에 저장

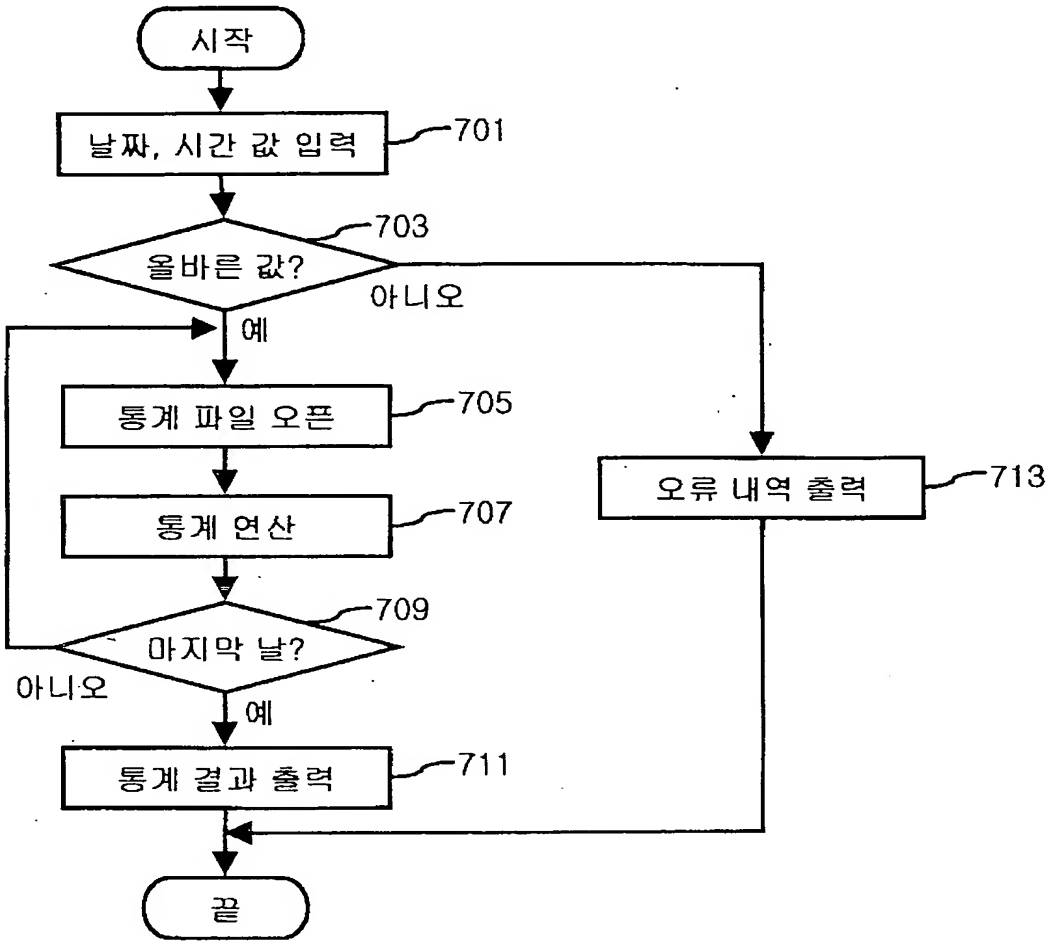
도면 5


시작
파일 저장 디렉토리 생성
501
버퍼링된 ./file 디렉토리 모니터링
503
설정 개수의 패킷이 저장 완료된 파일?
505
아니오
예
파일 오픈
507
각 패킷의 IP 헤더 추출
509
TCP 프로토콜 인가?
511
아니오
예
TCP 헤더와 사용자 데이터 추출
513
끝

도면 6


시작
601
날짜 변경?
예
603
새 통계 파일 생성
아니오
605
Finish 패킷?
예
607
해당 메모리 초기화
아니오
609
수신 시간 초과?
예
611
해당 메모리 초기화
아니오
613
기존 파일 패킷?
아니오
615
Header, Data File 오픈
예
617
메모리에 추가
621
통계 결과 파일 저장
끝

도면 7


시작
날짜, 시간 값 입력
701
703
올바른 값?
아니오
예
통계 파일 오픈
705
통계 연산
707
709
마지막 날?
아니오
예
통계 결과 출력
711
오류 내역 출력
713
끝